КАНЦЭПЦЫЯ ІНФАРМАЦЫЙНАЙ БЯСПЕКІ РЭСПУБЛІКІ БЕЛАРУСЬ

76. Разам з гэтым адным з прыярытэтных кірункаў дзейнасці ўпаўнаважаных дзяржаўных органаў з'яўляецца прафілактыка кіберзлачыннасці, заснаваная на папулярызацыі сярод насельніцтва, перш за ўсё моладзі, нецярпімасці да асацыяльных паводзінаў у інфармацыйнай прасторы, правядзенні растлумачальнай работы ў СМІ і сетцы Інтэрнэт у мэтах фарміравання бяспечнай нацыянальнай інфармацыйнай экасістэмы. Для павышэння правасвядомасці і зніжэння ўразлівасці ад кібератак праводзіцца навучанне грамадзян асновам паводзінаў у інфармацыйнай сферы.

РАЗДЗЕЛ VI ЗАБЕСПЯЧЭННЕ БЯСПЕКІ ІНФАРМАЦЫЙНЫХ РЭСУРСАЎ

ГЛАВА 20

Абумоўленасць мер па забеспячэнні бяспекі інфармацыйных рэсурсаў

77. З'яўленне шырокіх і даступных магчымасцяў для збору, захавання і апрацоўкі вялікага аб'ёму даных, стварэнне тэхналогій прамога доступу да інфармацыі абумоўліваюць неабходнасць разглядаць яе як самастойны і каштоўны рэсурс. Інфармацыйныя рэсурсы становяцца прыярытэтным аб'ектам злачынстваў і кіберінцыдэнтаў, падвяргаюцца выкраданню, мадыфікацыі, знішчэнню, блакіраванню і іншым уздзеянням.

78. Павышаецца значэнне тэхнічнай абароны інфармацыі абмежаванага распаўсюджвання, у той час як сродкі выкрадання, незаконнага блакіравання і іншага ўздзеяння на інфармацыйныя рэсурсы ўніверсальна прымяняюцца ў палітычных, ваенных, разведвальных, эканамічных, злачынных і іншых мэтах.

Множныя пагрозы і рызыкі незаконнага і неабгрунтаванага ўмяшання ў прыватнае жыццё грамадзян, выкраданне персанальных даных, кампраметацыя рэквізітаў доступу і залішняе прафіляванне звужаюць асабістую прастору чалавека і парушаюць яе прыватнасць. Раскрыццё асабістай інфармацыі стала неад'емным атрыбутам карыслівых злачынстваў і злачынстваў супраць асобы.

Фарміруецца нелегальны рынак баз і банкаў даных, попыт на якія абумоўлівае выкраданне інфармацыйных масіваў, якое суправаджаецца парушэннем аўтарскіх правоў.

ГЛАВА 21

Асноўныя кірункі забеспячэння бяспекі інфармацыйных рэсурсаў

79. Асноўнымі крыніцамі пагроз у галіне забеспячэння бяспекі інфармацыйных рэсурсаў у Рэспубліцы Беларусь трэба разглядаць дзейнасць асобных асоб, злачынных груп, нядобрасумленных айчынных і замежных арганізацый, аб'яднанняў ці супольнасцяў, накіраваную на атрыманне неправамернага доступу да гэтых рэсурсаў у палітычных, ваенных, камерцыйных, асабістых і іншых мэтах, які ажыццяўляецца ў абыход устаноўленага парадку або насуперак агульнапрынятым нормам маралі, а таксама парушэнне функцыянавання інфармацыйнай інфраструктуры.

80. Асноўнай мэтай дзяржаўнай палітыкі ў галіне забеспячэння бяспекі інфармацыйных рэсурсаў з'яўляецца захаванне іх даступнасці, цэласнасці і канфідэнцыяльнасці.

81. Сістэма забеспячэння бяспекі інфармацыйных рэсурсаў заснавана на стратэгічным прынцыпе захавання балансу свабоды інфармацыі і права на тайну, гарантыях дзяржавы на распаўсюджванне або прадастаўленне агульнадаступнай інфармацыі.

(Заканчэнне. Пачатак на 5—7-й стар.)

Дзяржава забяспечвае пашырэнне бяспечнага доступу да інфармацыйных рэсурсаў добрасумленных карыстальнікаў, развіццё сэрвісаў якаснага і зручнага прадастаўлення інфармацыі, удасканаленне сістэм яе даных.

82. На гэтым этапе неабходна галоўным чынам забяспечваць надзейную і ўсебакова абумоўленую абарону інфармацыі абмежаванага распаўсюджвання, бяспеку персанальных даных і дзяржаўных інфармацыйных рэсурсаў.

ГЛАВА 22

Абарона дзяржаўнай і службовай тайны

83. Бяспека даных, аднесеных да дзяржаўнай або службовай тайны, забяспечваецца ў адпаведнасці з нацыянальным заканадаўствам аб дзяржаўных сакрэтах. Пры дапамозе прававой забароны абмяжоўваецца абарачэнне інфармацыі, якая ўтрымлівае звесткі, аднесеныя да дзяржаўных сакрэтаў, атрыманне асобамі сакрэтных звестак. Выключаюцца захоўванне і апрацоўка звестак у агульнадаступных формах, у тым ліку ў інфармацыйных сістэмах, якія маюць доступ у сетку Інтэрнэт і іншыя адкрытыя камп'ютэрныя сеткі. Уводзіцца адказнасць за парушэнне прававой забароны і прадпісанняў у сферы дзяржаўных сакрэтаў.

84. Разам з гэтым аднясенне інфармацыі да дзяржаўных сакрэтаў з'яўляецца выключным правам строга вызначанага пераліку дзяржаўных органаў і арганізацый і ажыццяўляецца на падставе ацэнкі шкоды (урону) ад выдавання, выкрадання або страты такой інфармацыі. Арганізацыйныя, матэрыяльныя і іншыя выдаткі на забеспячэнне абароны гэтай інфармацыі не могуць перавышаць названай шкоды (урону), высновы аб магчымасці і памеры якой робяцца на аснове канкрэтных паказчыкаў (індыкатараў) або прынятых практык.

Дзяржава зыходзячы з прэзумпцыі свабоднага распаўсюджвання інфармацыі, а таксама з мэтай павышэння адкрытасці сацыяльна-эканамічных і іншых грамадскіх адносін зацікаўлена ў паслядоўным памяншэнні колькасці дзяржаўных органаў і арганізацый, надзеленых паўнамоцтвамі засакрэчвання інфармацыі, і агульнага аб'ёму дзяржаўных сакрэтаў з адначасовай гарантавана эфектыўнай абаронай звестак, якія ахоўваюцца. Пры гэтым не дапускаецца пашырэнне або ўзмацненне жорсткасці рэжымных мер, не абумоўленае сістэмнымі недахопамі ў сферы абароны дзяржаўных сакрэтаў, якія пацягнулі шкодныя наступствы.

85. Узнікае неабходнасць адаптацыі інстытута тайнаў да развіцця інфарматызацыі. Разам з арганізацыйна-прававымі мерамі забеспячэння бяспекі інфармацыі ўзрастае роля яе абароны і тэхнічнымі метадамі. У галіне тэхнічных і крыптаграфічных метадаў абароны дзяржаўных сакрэтаў максімальна ўлічваюцца наяўныя звесткі аб сродках, метадах, тэхналогіях атрымання несанкцыянаванага доступу да інфармацыйных рэсурсаў, якія ахоўваюцца, вынікі аператыўна-вышуковай і контрразведвальнай дзейнасці, навуковых даследаванняў і вопытных распрацовак, а таксама ўсебаковыя веды ў галіне сучасных ІКТ і асаблівасці абстаноўкі ў сферы нацыянальнай бяспекі.

Дзяржаўныя органы, надзеленыя паўнамоцтвамі па вызначэнні парадку абароны дзяржаўных сакрэтаў ад уцечкі па тэхнічных каналах, забяспечваюць яго адэкватнасць і суразмернасць магчымым рызыкам.

ГЛАВА 23

Бяспека інфармацыі абмежаванага распаўсюджвання і абарона персанальных даных

86. У адпаведнасці з нарматыўнымі прававымі актамі Рэспублікі Беларусь ажыццяўляюцца фарміраванне і абарона службовай інфармацыі абмежаванага распаўсюджвання, а таксама абарона інфармацыі, якая складае камерцыйную, прафесійную, банкаўскую і іншую тайну, якая ахоўваецца законам, інфармацыі аб прыватным жыцці фізічнай асобы, персанальных даных, іншай інфармацыі, доступ да якой абмежаваны заканадаўчымі актамі Рэспублікі Беларусь.

87. Ва ўмовах фізічнай немагчымасці і немэтазгоднасці цалкам аддзяліць інфармацыйныя сістэмы і рэсурсы, якія змяшчаюць гэтыя даныя, ад сеткі Інтэрнэт і іншых сетак агульнадаступнага карыстання фізічным і юрыдычным асобам неабходна ажыццяўляць неабходныя прававыя, арганізацыйна-распарадчыя і тэхнічныя меры, якія забяспечваюць мінімізацыю колькасці кіберінцыдэнтаў і шкоды ад іх у гэтых сістэмах.

88. Дзяржава ў сваю чаргу павінна ўдасканальваць патрабаванні да абароны інфармацыі, у тым ліку працягваць развіццё сістэмы пацвярджэння адпаведнасці сродкаў тэхнічнай і крыптаграфічнай абароны інфармацыі, а таксама ліцэнзавання дзейнасці ў галіне тэхнічнай абароны інфармацыі.

89. Дасягненне абароненасці персанальных даных забяспечвае ўзважаная дзяржаўная палітыка па вызначэнні патрабаванняў да разнастайных суб'ектаў інфармацыйных адносін, якія ажыццяўляюць збор, апрацоўку і захаванне гэтых даных.

Увага дзяржавы засяроджваецца на ўдасканаленні нарматыўнай прававой базы ў гэтай галіне. Дзяржаўнае рэгуляванне збору, апрацоўкі, прадастаўлення і распаўсюджвання персанальных даных ажыццяўляецца з улікам сучаснага міжнароднага вопыту, у тым ліку адпавядае палажэнням міждзяржаўных актаў. Падыходы да абароны персанальных даных, што фарміруюцца ў Беларусі, грунтуюцца на прынцыпе «бяспека па ўмаўчанні».

90. Важнай мерай па ўзмацненні кантролю ў гэтай сферы з'яўляецца функцыянаванне ў дзяржаве ўпаўнаважанага суб'екта (суб'ектаў) па абароне правоў фізічных асоб пры апрацоўцы іх персанальных даных.

ГЛАВА 24

Забеспячэнне бяспекі дзяржаўных інфармацыйных рэсурсаў і агульнадаступнай інфармацыі

91. Дзяржава забяспечвае абарону інфармацыйных рэсурсаў, якія знаходзяцца ў распараджэнні дзяржаўных органаў і арганізацый, ажыццяўляе прававое рэгуляванне карыстання, валодання і распараджэння інфармацыйнымі рэсурсамі. У гэтых мэтах ствараецца адзіная сістэма ўліку і захаванасці інфармацыйных рэсурсаў, а таксама прымяняюцца спецыяльныя працэдуры дзяржаўнай рэгістрацыі.

92. Дзяржаўнымі органамі ажыццяўляецца абарона агульнадаступнай інфармацыі ад супрацьпраўнага знішчэння, мадыфікацыі, блакіравання правамернага доступу, неабгрунтаванага засакрэчвання, утойвання, несвоечасовага распаўсюджвання ці прадастаўлення. Дзяржава забяспечвае забарону цэнзуры, гарантуе аператыўнае давядзенне агульнадаступнай інфармацыі вызначанымі заканадаўствам спосабамі, пашырае магчымасці адпаведных сэрвісаў, рэалізуе канцэпцыю «адкрытых даных». Дзяржава зацікаўлена ў падтрыманні балансу паміж патрэбай грамадзян у азнаямленні з агульнадаступнай інфармацыяй, іх права на адмову ад атрымання такой інфармацыі, а таксама неабходнасцю яе абароны ад супрацьпраўных замахаў.

РАЗДЗЕЛ VII МЕХАНІЗМЫ РЭАЛІЗАЦЫІ КАНЦЭПЦЫІ

ГЛАВА 25

Выкарыстанне палажэнняў Канцэпцыі пры падрыхтоўцы нарматыўных прававых актаў і іншых дакументаў

93. Палажэнні Канцэпцыі выкарыстоўваюцца пры падрыхтоўцы нарматыўных прававых актаў, дзяржаўных праграм, перспектыўных і бягучых планаў работы дзяржаўных органаў, у рэалізацыі праектаў залучаных грамадскіх арганізацый і ініцыятыў грамадзян, а таксама пры ацэнцы стану нацыянальнай бяспекі і ўдакладненні індыкатараў гэтага стану.

94. Распрацоўка і ажыццяўленне мер у галіне забеспячэння і ўмацавання інфармацыйнай бяспекі, якія адпавядаюць гэтай Канцэпцыі, грунтуюцца на навуковым забеспячэнні, уключаючы фундаментальныя і прыкладныя даследаванні, і выніках практычнай дзейнасці.

95. У галіне прававога забеспячэння інфармацыйнай бяспекі Канцэпцыя служыць асновай для спецыяльных актаў заканадаўства, якія вызначаюць прававое становішча суб'ектаў забеспячэння інфармацыйнай бяспекі, рэгулююць дзейнасць дзяржаўных органаў па яе забеспячэнні, фармулююць нормы і правілы правамерных паводзінаў у інфармацыйнай сферы, неабходныя рэгламенты, абмежаванні і забароны, замацоўваюць іншыя нормы па гарантаванні бяспекі інфармацыйнай сферы і абароненасці адпаведных інтарэсаў асобы, грамадства і дзяржавы.

ГЛАВА 26

Дзяржаўна-прыватнае партнёрства ў сферы забеспячэння інфармацыйнай бяспекі

96. Эфектыўнаму вырашэнню задач у забеспячэнні інфармацыйнай бяспекі павінна садзейнічаць пастаяннае мэтанакіраванае ўзаемадзеянне паміж дзяржаўным сектарам і камерцыйнымі арганізацыямі ў форме дзяржаўна-прыватнага партнёрства з мэтай прыцягнення кампетэнцый, кадраў, тэхналогій, капіталу прыватных прадпрыемстваў, павышэння аддачы выкарыстання бюджэтных сродкаў і актываў прадпрыемстваў, сумеснай распрацоўкі і рэалізацыі інвестыцыйных і іншых праектаў у галіне інфармацыйнай бяспекі.

97. Дзяржаўна-прыватнае партнёрства ў галіне забеспячэння інфармацыйнай бяспекі разглядаецца як юрыдычна аформленае супрацоўніцтва дзяржаўнага органа і суб'екта гаспадарчай дзейнасці недзяржаўнай формы ўласнасці, якое заснавана на аб'яднанні рэсурсаў і размеркаванні рызык, рэалізуецца для забеспячэння інфармацыйнай бяспекі з прыцягненнем прыватных інвестыцый і кампетэнцый.

98. Адным з найважнейшых кірункаў рэалізацыі дзяржаўна-прыватнага партнёрства ў сферы гарантавання інфармацыйнай бяспекі з'яўляецца падтрымка айчынных вытворцаў праграмнага забеспячэння інфармацыйных сістэм і сістэм інфармацыйнай бяспекі.

Нароўні з пераадоленнем залежнасці Беларусі ад іншых краін — вытворцаў праграмных і апаратных сродкаў рэалізацыя інфраструктурных праектаў і праектаў, непасрэдна звязаных з забеспячэннем інфармацыйнай бяспекі праз механізм партнёрства дзяржавы і айчынных прыватных кампаній, павінна спрыяць фарміраванню рынкавага попыту на імпартазамяшчальную нацыянальную інфармацыйна-тэхналагічную прадукцыю, павышэнню яе якасці.

99. Дзяржава зацікаўлена ва ўзаемадзеянні з ІТ-кампаніямі, інтэрнэт-правайдарамі, аператарамі сувязі і знешнімі экспертамі ў абнаўленні і развіцці механізмаў выяўлення пагроз інфармацыйнай бяспецы праз ІТ-аўдыт, маніторынг кіберрызык, пошук уразлівасцяў і актуальных сродкаў абароны, выпрацоўку правілаў паводзінаў у сетцы Інтэрнэт.

100. Дзяржаўна-прыватнае партнёрства спрыяе падрыхтоўцы кваліфікаваных кадраў у галіне інфармацыйнай бяспекі, фарміраванню актуальных праграм падрыхтоўкі адпаведных спецыялістаў, укараненню новых адукацыйных і прафесійных стандартаў у гэтай сферы, а таксама павышэнню агульнай камп'ютарнай адукаванасці насельніцтва, уключаючы навучанне людзей старэйшага і сярэдняга ўзросту камп'ютарным навыкам, правілам карыстання персанальнымі данымі, уменню бяспечнай работы ў сетцы Інтэрнэт.

101. У сувязі з трансфармацыяй грамадскіх адносін у інфармацыйнай сферы дзяржаўна-прыватнае партнёрства становіцца найбольш эфектыўнай мадэллю забеспячэння інфармацыйнай бяспекі. У ёй дзяржава вызначае мэты, стратэгічныя задачы і рэгулятыўныя падыходы, а бізнес-супольнасць прадастаўляе тэхналогіі, веды і рэсурсы для вырашэння пастаўленых задач. Пры гэтым дзяржава імкнецца гарантаваць тэхналагічную нейтральнасць і абарону прыватных арганізацый (і іх інвестыцый) ад магчымых рызык.

ГЛАВА 27

Удзел Рэспублікі Беларусь у забеспячэнні міжнароднай інфармацыйнай бяспекі

102. Мэтай забеспячэння міжнароднай інфармацыйнай бяспекі з'яўляецца выяўленне, папярэджанне і нейтралізацыя знешніх рызык, выклікаў і пагроз інфармацыйнай бяспецы. Міжнароднае супрацоўніцтва ў сферы інфармацыйнай бяспекі на рэгіянальным, двухбаковым, шматбаковым і глабальным узроўнях накіравана на зніжэнне рызыкі выкарыстання інфармацыйных і камунікацыйных тэхналогій для ажыццяўлення варожых дзеянняў і актаў агрэсіі ў дачыненні да Беларусі.

103. У рамках забеспячэння міжнароднай інфармацыйнай бяспекі ажыццяўляецца актыўнае, усебаковае, узаемавыгаднае міжнароднае, у тым ліку міжведамаснае, супрацоўніцтва.

Забяспечваецца ўдзел Рэспублікі Беларусь у міжнародных арганізацыях, профільных міжнародных дагаворах, двухбаковых адносінах з іншымі дзяржавамі, у іншых формах міждзяржаўнага супрацоўніцтва ў мэтах фарміравання механізмаў міжнароднага ўзаемадзеяння па супрацьдзеянні пагрозам міжнароднай інфармацыйнай бяспецы.

104. Галоўным сродкам для дасягнення мэт забеспячэння міжнароднай інфармацыйнай бяспекі з'яўляюцца падтрымка і прасоўванне адпаведных ініцыятыў, якія адпавядаюць нацыянальным інтарэсам Рэспублікі Беларусь у інфармацыйнай сферы.

Беларусь падтрымлівае прасоўванне мер даверу ў сферы міжнароднай інфармацыйнай бяспекі і выступае за адказныя паводзіны дзяржаў у інфармацыйнай сферы, якія прадугледжвалі б у першую чаргу прадухіленне ў ёй канфліктаў, а не іх урэгуляванне. Дзяржавы павінны ўстрымлівацца ад мэтанакіраваных дэструктыўных інфармацыйных уздзеянняў на іншыя краіны, выключаць выкарыстанне сваёй тэрыторыі для ажыццяўлення кібератак, а таксама процідзейнічаць выкарыстанню схаваных шкодных функцый і праграмных уразлівасцяў у праграмна-апаратных сродках, дабіваючыся іх бяспекі для карыстальнікаў.

105. Рэспубліка Беларусь прымае ўдзел у міжнародным інфармацыйным абмене на аснове міжнародных дагавораў і пагадненняў, у рамках юрысдыкцыі — гарантуе яго бяспеку.